Viatores® Mobile VPN Technical Overview

ECUTEL®

Publication Date: December 2003 (Revision 4.0. Last updated: February 9, 2004).

Ecutel Systems, Inc.
2300 Corporate Park Drive
Suite 410
Herndon, VA 20171, USA

Phone: +1-571-203-8300
Fax: +1-571-203-8310
Web: www.ecutel.com

Table of Contents

Introduction

Mobile products and services are designed to increase the productivity of mobile professionals. As these solutions evolve and proliferate, however, enterprise IT managers are faced with numerous challenges related to maintaining network security while providing the required support for their users. If IT managers lag behind the curve, users tend to take matters into their own hands as demonstrated by the popularity of personal PDA devices and rogue wireless LAN access points around the offices of most corporations today. Although PDA devices might be personal, sensitive corporate information can easily end up being transmitted from them. Rouge or insecure wireless LAN access points are the equivalent of security holes in the corporate firewall.

In theory, business users should be able to have access to corporate network resources regardless of where they are. If they are in the office, they should be able to use a wired or wireless LAN. If they are on the road, they should get access to the same resources using hot spots or wide-area wireless networks such as GPRS or 1xRTT. If they are at home, they should be able to connect using their Digital Subscriber Line (DSL) or cable modem. From an IT perspective, all these connections must be secure and easy to use in order to reduce support cost. Viatores makes this a reality. It provides proven security, seamless roaming, and easy management.

Viatores is a mobile Virtual Private Network (VPN), a next-generation VPN designed specifically for enterprises with mobile professionals. With Viatores, IT managers are assured that their wireless LAN implementation is secure and that connections made by users' mobile devices outside the office do not compromise the corporate network. In the office, users unplug from the LAN and automatically connect to the wireless LAN when they leave their desks. Viatores makes the transition from the LAN to the wireless LAN seamless and secure, turning on encryption automatically when the wireless LAN is used. On the road, users can connect to their corporate network securely using any available connection, wired or wireless, including hot spots and wide-area wireless networks. Finally, users can connect from home using their broadband connection of choice.

The underlying protocols on which Viatores relies are Mobile IP and IPSec in accordance with the IETF RFCs 2002, 2003, 2005, 2006, and 2344. The intent of Mobile IP was to establish a standard to allow seamless network traversal so that mobile users could experience ubiquitous communications. IPSec is the security standard of choice for the vast majority of VPNs. However, unlike legacy VPNs, Viatores provides seamless mobility based on the Mobile IP standard while maintaining security regardless of where the user connects from.

Viatores' architecture is scalable and flexible. The problem of an expanding list of mobile computing devices and communications infrastructures led the Ecutel team to create an architecture that is positioned for today's environment as well as tomorrow's. Viatores can easily support new communication networks, such as 3G and Bluetooth.

Viatores Mobile VPN unique features include the following:

- Trusted security of IPSec, Mobile IP and other proven standards
- Seamless roaming and application persistence
- Automatic selection of best available network
- Optimized and policy-driven security
- Single sign-on network login and pre-boot security
- Integration with existing network infrastructure
- Vendor-independent security solution allows interoperability between the different Wi-Fi hardware vendors
- Support for all wireless networks: Wi-Fi, GPRS, 1xRTT, eVDO, CDPD, PHS, and many others
- Hardware-based acceleration and clustering for scalability.

This technical overview provides detailed information on the above features.

Viatores Overview

Viatores is a client-server mobile virtual private network (VPN) software that provides enterprises with intelligent security and optimized mobility inside and outside the office. It includes features traditionally found in legacy VPNs such as strong encryption and authentication security based on the IPSec standard. However, while legacy VPNs are designed for either point-to-point connections or stationary users connecting from remote locations, Viatores was designed specifically for the mobile workforce from the ground up. Its mobility features are based on the Mobile IP standard to provide users with an always-on, secure connection to the corporate networks, regardless of where they connect from or how.

Viatores is designed for enterprises with mobile security needs internally (within the corporate network) and externally (through remote public and private networks).

With Viatores, mobile workers can use a variety of devices to maintain a secure connection to corporate resources while roaming inside and outside the office. This means they can instantly send and receive email, retrieve information stored on corporate networks, or participate in Net meetings -- regardless of location. And if the mobile worker moves during a session forcing a change in network, Viatores maintains the application session so that work can continue uninterrupted without any reconfiguration, rebooting, or restarting of the programs in use.

Viatores enables mobile devices to roam between private networks, public networks and private visiting networks seamlessly and securely using a variety of communication networks including:

- Wireless and Wired LANs
- Virtual LANs
- Wireless and Wired Public Networks

With the advantage of continuous connectivity, the productivity of mobile professionals increases dramatically. Members of mobile workgroups can collaborate efficiently, and executives can stay connected to corporate resources easily and in real-time. Because Viatores users maintain the same network address regardless of the network they connect from, they can be reached by any peer-to-peer application such as video-conferencing.

Viatores Components

The Viatores architecture was built with complete network flexibility in mind. Regardless of how your network is configured, or where or how users access your corporate network, Viatores can be configured to suit your needs. To accomplish this Viatores comprises

multiple server components that can be set up according to your network and roaming needs. A typical configuration comprises of a Viatores Server and a Viatores Gateway.

Viatores Server

The Viatores Server is the core server component of the Viatores system. It resides within the corporate network and is responsible for several tasks including encryption, authentication, and traffic management. The Server performs these tasks by recognizing individual IP packets and their destinations. Once it is determined that the device to whom the IP packet is directed is not physically attached to the home network, the IP packet is automatically re-routed and sent to the device's current point of network attachment via the IP address associated with its new location, known as *care-of* IP address. The Server ensures that data remains secure through the formation of an authenticated and encrypted IP tunnel that is IPSec compliant. This component combines the functions of a Mobile IP home agent and an IPSec VPN server.

Viatores Gateway

The Viatores Gateway is located in the public Demilitarized Zone (DMZ) of the corporate network. This component provides a flexible and portable mechanism for secure firewall traversal. It accepts IP-in-IP and UDP traffic from the Viatores Client and authenticates it before forwarding it across the firewall to the Viatores Server.

Viatores Relay Point

The Viatores Relay Point is an optional component that can be installed on internal subnets if Dynamic Host Configuration Protocol (DHCP) is not used on that subnet. If used, the Viatores Client will use the Relay Point's IP address as a care-of address instead of a dynamically assigned one to attach to the network. This component is known as "foreign agent" in Mobile IP terminology. The Viatores Client is said to operate in *co-located* mode when a Relay Point or another Mobile IP foreign agent does not exist on the visited network.

Viatores Client

The Viatores Client is installed on mobile devices running the Windows operating system or Pocket PC. It is responsible for network device discovery, communication with the server components, authentication, and encryption/decryption.

Viatores Manager

The Viatores Manager is used by network administrators for user and server configuration, key management, and policy distribution. This component can reside on any secure machine and can communicate the configuration and key details to the Server, Relay Point, Gateway, and individual Clients.

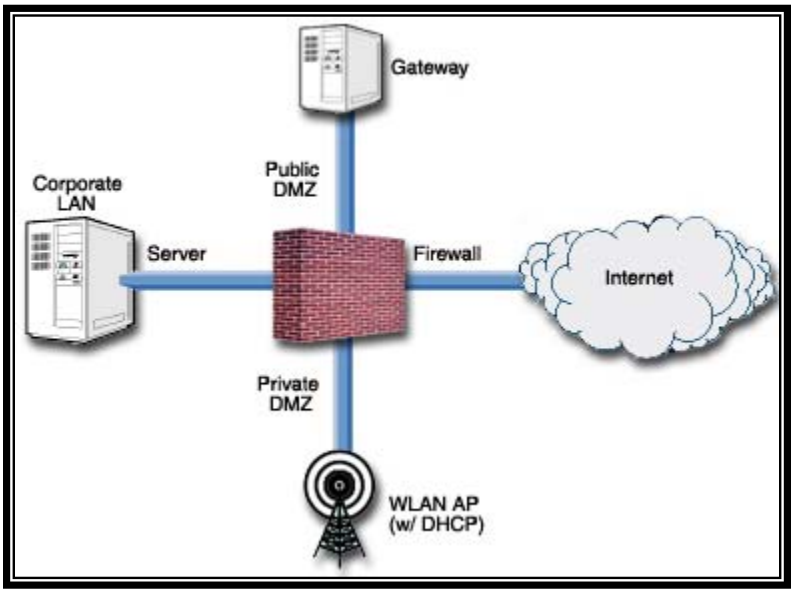

Figure 1

The diagram above shows a typical Viatores implementation where the Viatores Gateway is placed in the public DMZ (along with other public devices such as the web server, SMTP relay, etc…) and the wireless LAN access points are placed in a private DMZ. The firewall is configured to allow Mobile IP IP-in-IP and UDP traffic between the private DMZ and the Viatores Gateway only and Mobile IP IP-in-IP traffic between the Viatores Gateway and the Viatores Server. This way, the wireless LAN subnet is treated as a public network and non-Viatores traffic is disallowed from that subnet. Optionally, the firewall can be configured to allow HTTP traffic from the wireless LAN subnet to the Internet directly to give visitors web access.

Viatores Architecture

Viatores' core architecture relies on two standards, IPSec and Mobile IP, for security and mobility, respectively. The details of these two standards are published by the Internet Engineering Task Force (IETF) under the following Request for Comment (RFC) documents: 2002, 2003, 2005, 2006 and 2344, which are available to the public.

The choice for a standards-based architecture is not accidental. The two standards employed in Viatores have been publicly scrutinized by the engineering community and are considered to be very reliable, especially as they relate to security. Solutions that are not based on standards and rely on proprietary security and mobility schemes are typically weak or poorly implemented. Their architecture has never been scrutinized by the public.

TCIP/IP Interface

Viatores is designed to ensure data packets are efficiently and securely exchanged between a mobile device and a home network server or another mobile device, regardless of network attachment. Viatores allows this exchange to proceed securely and transparently to the user. For this purpose, Viatores manipulates the IP addresses and IP packets so that end-to-end connection between two peer applications is maintained as the Client roams through heterogeneous communication networks, traverses different IP domains, or is stationary in a remote site.

Viatores operates at the network layer of the TCP/IP stack (see Figure 2). The network layer is the most logical place for Viatores because it is far enough above the link layer to remain independent of the physical link. Placing key features at this point enables Viatores to recognize network operations and to then transition between them as deemed necessary. Also, Viatores' placement in the network layer means it is far enough below the application layer to avoid any inefficiency that might be experienced if placed higher or lower in the stack. In this regard, the Viatores Server performs intelligent data packet recognition, mapping, tunneling, encryption, compression, and forwarding while maintaining transparency for TCP/IP applications.

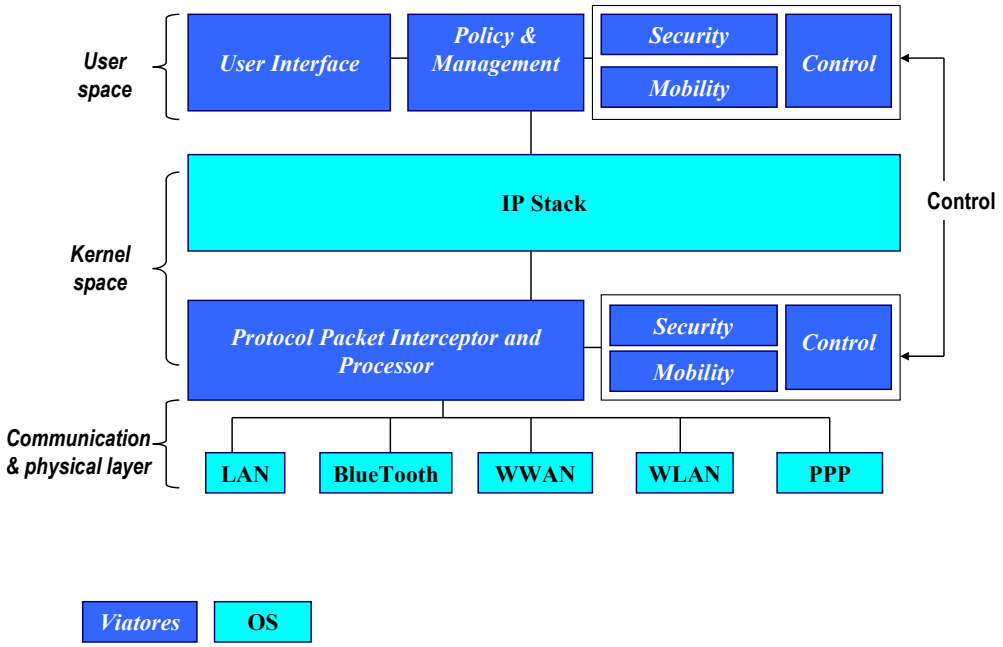

Figure 2

Registration and Authentication

The Viatores Server supports multiple user authentication mechanisms including local authentication using the Viatores Server user database, Microsoft Active Directory, LDAP, RADIUS, and RSA SecurID. Each Viatores user must be authenticated on the Server using one or more of the above methods for maximum security. In addition, Viatores requires an additional level of registration authentication using one of two methods: shared secrets or Public Key Infrastructure (PKI) certificates. A combination of user authentication and registration authentication ensures the highest level of security for all Client-Server communication.

Client Registration

The Viatores Server periodically transmits broadcast messages, or agent advertisements, and waits for registration/de-registration request messages from other Viatores components, such as the Viatores Client. Such request messages can be received directly from any Client operating in co-located mode or indirectly through a Relay Point or a Mobile IP foreign agent, if one exists on the visited network. The Client registration message provides a means to allow the mobile device to authenticate to the Viatores Server using the Mobile IP protocol. The Mobile IP registration message is protected with keyed MD5 hashing based on pre-shared secret known only between the Viatores Client and Viatores Server. As part of Client registration, it also informs the Viatores Server of its current location.

The Viatores Client must inform the Server of its current location by providing a care-of, or forwarding, IP address that the Server uses for relaying traffic sent to the Client's permanent IP address. The Client registers with the Server by sending to the Server either a registration request with a new address, a registration renewal confirming the current address, or a de-registration upon return to the home network. The registration process is performed periodically dependent upon a *time interval value* set by the network administrator in the Viatores Server.

The Viatores Client continuously listens to broadcast messages that are frequently sent by the Server. The Client is capable of listening to these broadcasts through all physical interfaces, empowering it with seamless and transparent traffic switching.

Registration Security

Viatores strictly adheres to the ISAKMP and Internet Key Exchange (IKE) protocol standards. This ensures that the security association exchanged and the interoperability between any two Viatores communication end points is versatile enough for dynamic mobility, yet security parameters remain uncompromised. This approach ensures Viatores interoperability with other products that adhere to this standard.

IKE requires two distinct phases in the establishment of security associations. The first phase serves two purposes. First, the negotiating parties authenticate each other and, second, they negotiate an intermediate security association (ISAKMP SA) to protect the second phase. The IKE second phase is used to negotiate security association to derive symmetric keys to protect all future IP traffic with encryption, decryption and integrity.

Shared Secrets

The Viatores Manager generates unique shared secrets for the individual Clients. All shared secrets are encrypted by a pass phrase (password), stored in the Manager's database and, accessible only by the Manager. When shared secrets are distributed to individual Viatores components, they are in the form of *blobs*, an unrecognizable series of characters, strongly encrypted based on a pass phrase. Shared secrets can be distributed along with the user's unique configuration files on a floppy disk, smart card, SEIS V2 Electronic ID Card, and other such devices. They can also be retrieved from the Viatores Server by the Viatores Client automatically. Upon logging in to the Viatores Client, the user will be required to provide the credentials to authentication system used (i.e. local, Active Directory, etc…) and the password to the shared secret. Depending on the configuration used, the user may provide the credentials using the Windows domain login screen or Graphical Identification and Authentication (GINA).

Certificates

The use of PKI certificates provides a higher level of authentication security than shared secrets. Viatores provides an infrastructure for supporting PKI certificates for organizations equipped with supporting certificates.

The Viatores PKI infrastructure provides for the efficient distribution of digital certificates containing public keys. With this approach one party can authenticate itself to the other by proving that it possesses the private key that corresponds to the public key on the certificate. The signature of the Certificate Authority (CA) provides proof that the certificate itself is legitimate.

To provide strong and scalable authentication during IKE negotiations, digital certificates and the PKI are used. A successful IKE registration is required to gain access to the services of the Viatores Server and, therefore, the home network. Consequently, the strong authentication provided by the use of PKI extends to the entire Viatores system.

Principally, digital certificates in X.509 v3 format are used as a means to produce authenticators through the use of digital signature algorithms. Standard certificates are issued by a CA to Clients and Servers for use in IKE protocol phase 1. Viatores components interpret the contents of certificates to extract pertinent information. Most importantly for IKE, the public key of the other party is extracted and used to verify that the other party possesses the corresponding private key.

Authentication would not be complete unless the authenticity and validity of the certificate itself can be verified. For that purpose, Viatores components can interact with the PKI to check that the certificate is not expired or revoked and that it has been issued by a trusted entity (Certificate Authority). Since Viatores relies on standard certificates, other applications can use the same certificates. In other words, Viatores can leverage off an existing PKI.

User Authentication

In addition to having a shared secret or a PKI certificate installed on their mobile device, users must provide login credentials to access a Viatores-enabled network. Login credentials typically include a combination of a username and password. Network administrators specify the user authentication method to be used by the end users using the Viatores Managers. The user authentication method can be specified globally or on a per user group basis.

Viatores User Local Database

If local authentication is used, the administrator can add user's to the Viatores local user database and specify their passwords. In this case, users will be required to provide a username and password when the Viatores Client starts. In this case, the username and password may or may not be the same as the Windows login credentials.

When local authentication is used, credentials provided by users during login are checked against the Viatores Server local user database.

Windows Active Directory

If an organization uses the Windows Active Directory, the network administrator can add users or groups directly from Active Directory. In this case, credentials provided by users during login are checked against the Active Directory server.

If Active Directory is used for Viatores user authentication, the Viatores Client can be set up to start automatically using the same credentials provided by the user to login to the Windows network. This option is called *single sign-on*.

RADIUS

If an organization uses RADIUS for user authentication, login credentials are checked against the RADIUS server specified by the network administrator during the initial set up of Viatores.

RSA SecurID®
RSA SecurID is a two-factor authentication scheme. It is based on something a user knows (a password or PIN), and something a user has (an authenticator) — providing a much more reliable level of user authentication than reusable passwords.

If SecurID authentication is used, the user will be prompted to enter their SecurID one-time password after the initial Viatores login process.

Data Encryption & Integrity

The Viatores Server and Client encrypt and authenticate each datagram exchanged between the Viatores components as specified in the IPSec standard. This in effect establishes secure tunnels between any two end points, regardless of where the user connects from or how.

Client–Server Tunnel

Upon successful registration, an IP tunnel is established between the Server and the Client. This tunnel acts as a *logical link* connecting the Client directly to its home network. Tunnels are constructed by employing IP-in-IP encapsulation, a method by which a new IP header is appended to the original datagram. Tunneling is always required for the Server to relay packets from the home network to a roaming Client. Reverse tunneling is optional, but is recommended because it provides significant benefits that make it attractive in a security conscious environment.

The Client sends a hashed time-progressive registration to the Server to be authenticated before it can register with the home network. If the policy set by the system administrator requires security to be used, the Client establishes an IPSec tunnel with the Server through IKE and obtains symmetric keys. Viatores combines header information of Mobile IP (IP-in-IP) with the IPSec packet specification and places them in the same packet structure while strictly adhering to relevant IETF drafts and standards. This ensures that Viatores can perform the necessary mobility and security functions. Ecutel designed Viatores with logical layering of Mobile IP and IPSec modules in the kernel level to enable sequential processing of mobile traffic, which significantly increases processing efficiencies.

Reverse Tunneling

Viatores uses reverse tunneling to increase the security of traffic between the Client and the Server. The reverse tunnel is formed to allow end-to-end confidentiality and network protection based on source IP routing. The reverse tunnel is also used to traverse public address space to private address spaces (i.e. home network). Encapsulation and tunneling of traffic are necessary to properly route traffic across this boundary.

Remote Access Security

The Viatores Gateway is used to support connections from outside the firewall (i.e. from users roaming outside the office). In some instances, the Gateway is used to support internal subnets that are isolated from the rest of the corporate network, such as a wireless LAN subnet of the private DMZ as depicted in Figure 1 above. Unlike the Viatores

Server and Viatores Relay Point, the Viatores Gateway does not send out broadcast or Mobile IP agent advertisements.

The Viatores Gateway does not send out broadcast or agent advertisement messages like the Server. Rather, it accepts incoming traffic from the Client and records information about which Server the Client is associated with as part of the registration packet. Subsequently, it securely forwards all data packets to the proper Server through the firewall. When the Viatores Gateway is used, the secure IPSec tunnel between the Viatores Client and Viatores Server remains intact as the Viatores Gateway decapsulates and encapsulates IP packets with proper tunneling IP header information to enable traffic between Clients and Servers to securely traverse across the firewall.

The Gateway accepts Client traffic encapsulated in IP-in-IP or UDP.

IP-in-IP Encapsulation
IP-in-IP encapsulation is the default encapsulation method for Client-Gateway communication. This encapsulation method is used any time the Client is present in a network with routable or public IP addresses.

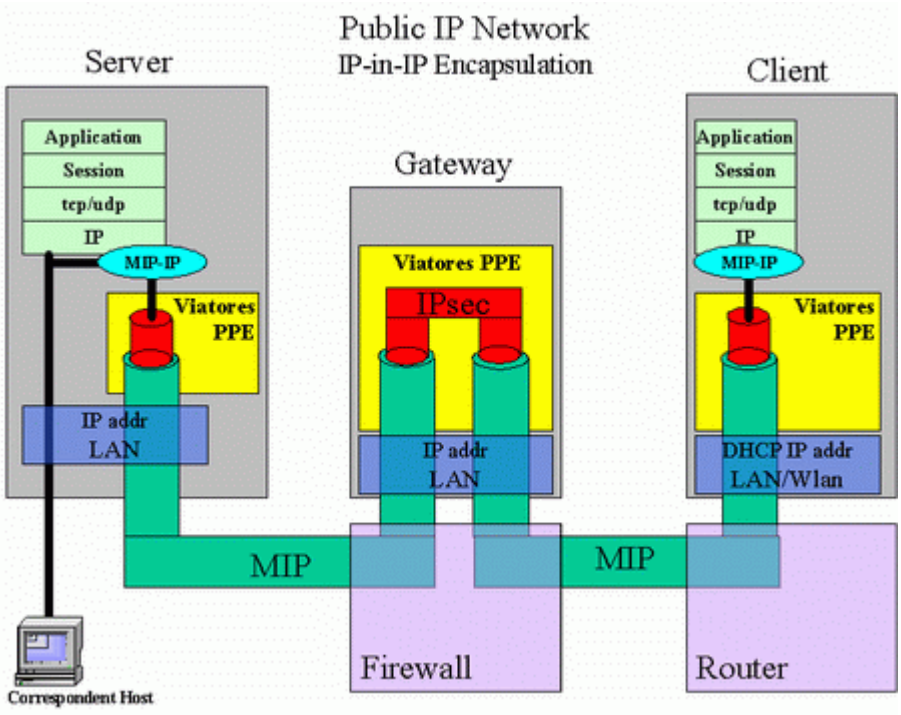

Figure 3: IP-in-IP Encapsulation

UDP Encapsulation
UDP encapsulation is used when the Client roams to private networks using Network Address Translation (NAT). In such networks, IP-in-IP traffic is not possible and therefore, the Client automatically recognizes this condition and provides UDP encapsulation over MIP and IPSec traffic to send to the Viatores gateway.

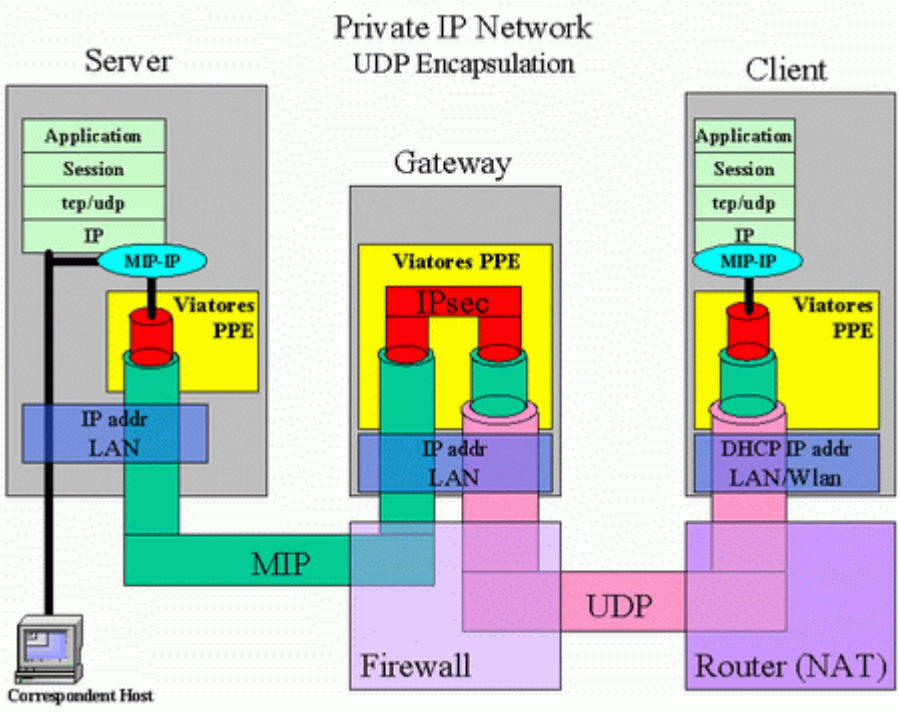

Figure 4: UDP Encapsulation

Optimized Mobility

Viatores' mobility features are based on the Mobile IP standard. However, as previously mentioned, the Mobile IP standard by itself does not address security related issues such as data encryption and integrity. Therefore, Viatores uses the IPSec standard to address these security issues.

The unique way in which Viatores combines the mobility and security for the mobile user results in *optimized mobility*, encryption is enabled only when required. This conserves processing resources on the Client and the Server. Figure 5 below shows a Viatores Client on the home LAN. In this case, Viatores detects its presence on the LAN and disables the encryption. Similar policies can be set for other adjacent subnets that are secure.

Viatores provides additional network-specific optimization capabilities including compress for low bandwidth networks as well as traffic shaping capabilities that can restrict the use of specific networks to an approved list of applications.

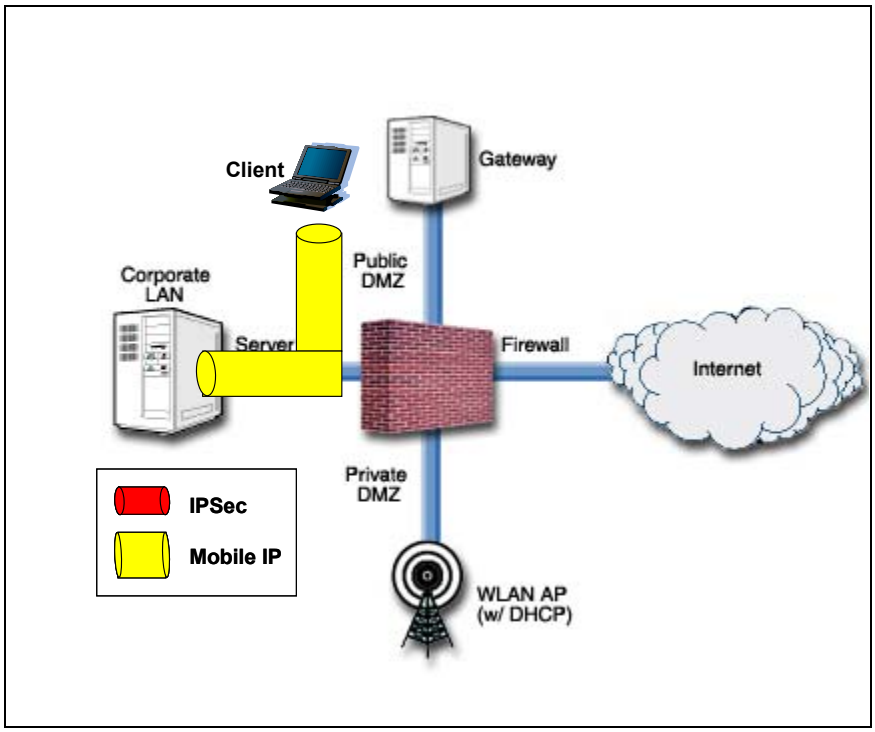

Figure 5: Client on home LAN – no encryption

In Figure 6 below, the Viatores Client has moved to the WLAN subnet which requires security. In this case, the Client automatically turns the encryption on. Similar security policy can be enabled for all untrusted networks, including the Internet.

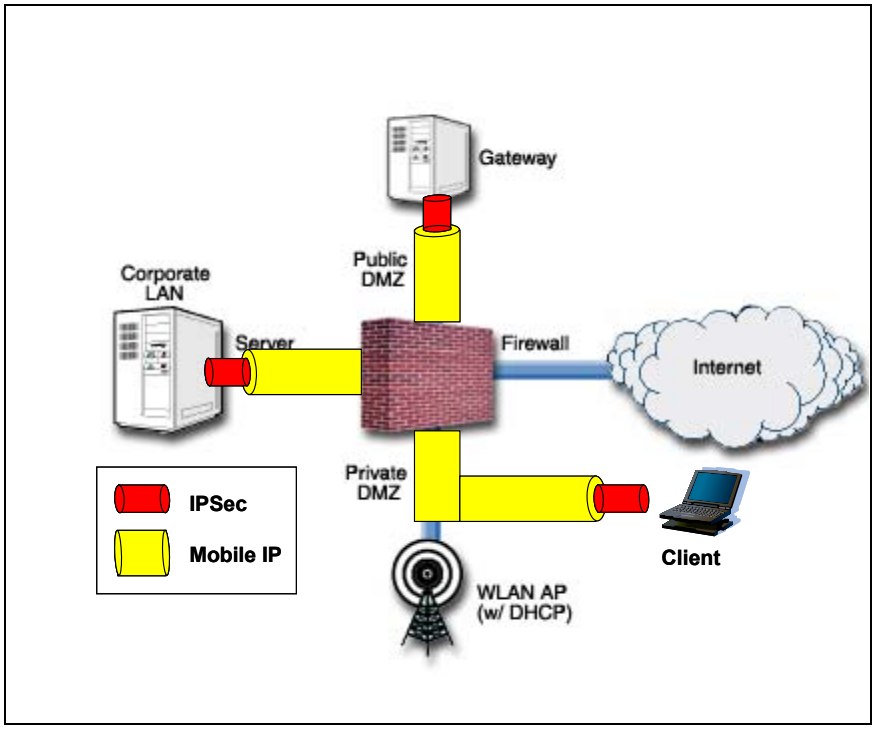

Figure 6: Client on WLAN – IPSec is enabled

Whenever Viatores detects multiple available networks to communicate over, it will select the one that offers the best connection to its Server based on the policies selected by the network administrator

Viatores Scalability

Scalability in the enterprise network environment must be concerned not only with network availability and performance, but also with the ability to support the growing and dynamic user base. Viatores addresses all three scalability issues.

Hardware Acceleration

Viatores supports hardware acceleration to improve overall system performance for large organizations. The optional hardware acceleration PCI card is designed to offload processing intensive encryption functions (such as DES, 3DES, and AES) and message integrity (such as MD5 and SHA-1) from the host server to improve performance and throughput. Hardware acceleration cards are available from Ecutel for systems with 33 MHz or 66 MHz buses and with encrypted throughput of up to 290 Mbps.

User/Key Management

One of the biggest headaches for IT departments is the deployment of technologies that require management of software on client computers. The IT department must worry about deploying this technology to an existing user base, then deploys it for every new user that is added to the enterprise. Furthermore, as new users come and go, and changes are necessary to the configuration, this problem is compounded. This problem is even made worse in a mobile environment where users are constantly on the road.

The Viatores Manager was designed to take the hassles out of network management for mobile enterprises by providing scalable, easy-to-use user and key management tools. The Manager allows network administrators to enable existing users in an Active Directory, for example, to be Viatores-enabled with very little effort. Configuration and security information can be retrieved by the Client directly from the Manager. This reduces the amount of work necessary to deal with each of the mobile clients.

Fail-over Capability

Network availability is of paramount importance whether the user is on the home network or visiting clients out on the road. In an enterprise network environment, Viatores offers the ability to configure redundant Servers with similar configurations and

duplicate Client keys. In the event of system failure continued network operation is ensured without the network administrator's intervention.

The Viatores fail-over capability enables the primary and secondary Servers of the fail-over cluster to maintain synchronized Mobile IP registration and IPSec Security association states. If one Server fails for whatever reason, the backup Server will immediately take over control to serve mobile Clients. During this transfer of control between fail-over Servers, the Client Mobile IP and IPSec tunnels remain intact and continue to support user roaming and communication without any interruption.

Viatores Specifications

Supported Hardware, Software, and Network Platforms

Server: Windows 2000, Windows 2003 and Linux.
Client: Windows 98, ME, 2000, XP, and Pocket PC.
Communication Networks: LAN (Ethernet), VLAN, Wireless LAN (802.11a/b/g), GPRS, GSM-Data, EDGE, CDPD, HSCSD, CDMA-One, 1xRTT, eVDO, D-AMPS, DoCoMo, PHS, POTS, ISDN, DSL, Cable, Public Safety radio (EDACS, OpenSky)

For the latest hardware/software compatibility list, check the Ecutel Web site at the following URL: www.ecutel.com

Security Features

Viatores supports a variety of encryption, authentication, and data integrity security features, including:

Data Confidentiality & Integrity
- Encryption using DES, 3DES, AES
- Pre-Shared Key (PSK)
- Public/private key X.509 certificates – RSA & DSA digital signatures

User Authentication Options
- Active Directory
- LDAP
- RADIUS
- Viatores local database
- RSA SecurID®

Client Security
- Compatibility with Wireless Protected Access (WPA) and 802.1x
- Always-on IP filtering security

Summary

The Viatores solution satisfies the demands of end users for seamless access to network resources, and meets the requirements of network administrators for a solution that is secure and easy to deploy and manage.

The Viatores software architecture is based on such standards as Mobile IP and IPSec, which provide an open and flexible solution that can work with other standards-based technologies. Viatores functions are grouped in an object-oriented fashion, and its interfaces are well defined for easy incorporation of new functions.

Viatores was designed to offer advanced routing, mobility, and security protocols, which enable it to transparently and fluidly traverse heterogeneous networks. Additionally, IP roaming is available complete with spontaneous, real-time information exchange that remains secure at all points along the packets route.

The features and capabilities provided by Viatores can benefit users of all mobile devices including laptop computers, personal data assistants, and smart phones; all operating in various heterogeneous networks, including LANs, wireless LANs, packet data wireless services, ISPs, and third generation mobile networks.

To find out if you qualify for a trial, visit Ecutel's Web site at the following URL: www.ecutel.com

About Ecutel Systems

Ecutel Systems is a pioneering provider of standards-based, secure enterprise mobility software. The company's technology brings seamless mobility to all facets of the enterprise, from simple and secure access for mobile workers to remote management for IT professionals.

The company's products include Viatores Mobile VPN for enterprise mobile security and Infrastructure Command & Control (IC^2) for mobile enterprise management.

For more information about Ecutel Systems, visit our Web site at the following URL: *www.ecutel.com*

Ecutel Systems, Inc.
2300 Corporate Park Drive, Suite 410
Herndon, VA 20171, USA
Tel: +1-571-203-8300
Fax: +1-571-203-8310
Email: info@ecutel.com